PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-274787
(43)Date of publication of application : 05.10.2001

(51)Int.Cl. H04L 9/08
G09C 1/00

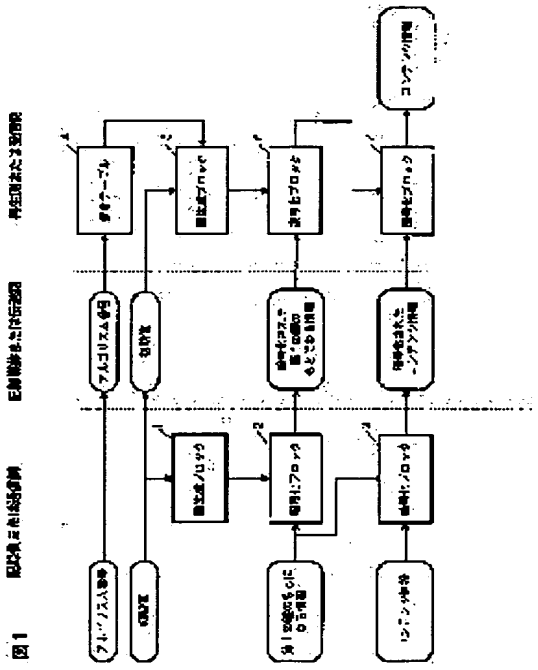
(21)Application number : 2000-051205
(22)Date of filing : 28.02.2000

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : KUROIWA TOSHIO
SUGAWARA TAKAYUKI
IBA WATARU
UEDA KENJIRO
HIGURE SEIJI

(30)Priority
Priority number : 2000012735 Priority date : 21.01.2000 Priority country : JP

(54) CONTENTS INFORMATION DECODING METHOD, CONTENTS INFORMATION DECODER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents information decoding method and a contents information decoder, by which a decoder side cannot respectively identify key generating algorithms used for encryption according to each designated algorithm number, only with the intelligence given to an encryption side, so as to more strongly prevent unauthorized reproduction and copy of contents information thereby enhancing copyright protection.
SOLUTION: The method and the decoder adopt decoding of encrypted contents information resulting from encrypting contents information, by using a 1st key generated from source information of the 1st key, source information of an encrypted 1st resulting from encrypting source information of the 1st key, using a 2nd key generated by a prescribed key generating algorithm on the basis of a given initial value, algorithm identification information for identifying the prescribed key generating algorithm and initial value information denoting the initial value.



LEGAL STATUS

[Date of request for examination] 27.09.2002
[Date of sending the examiner's decision of rejection] 03.02.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００１－２７４７８７
(P２００１－２７４７８７A)
(43)公開日　平成13年10月5日(2001.10.5)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
H04L	9/08		G09C	1/00	610 Z	5J104
G09C	1/00	610	H04L	9/00	601 A	9A001
					601 B	

審査請求　未請求　請求項の数8　OL　（全9頁）

(21)出願番号　特願2000-51205(P2000-51205)

(22)出願日　平成12年2月28日(2000.2.28)

(31)優先権主張番号　特願2000-12735(P2000-12735)
(32)優先日　平成12年1月21日(2000.1.21)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町3丁目12番地
(72)発明者　黒岩　俊夫
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内
(72)発明者　菅原　隆幸
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内
(72)発明者　猪羽　渉
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内

最終頁に続く

(54)【発明の名称】コンテンツ情報復号化方法、コンテンツ情報復号化装置

(57)【要約】
【課題】　暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリズム番号に従って暗号化に用いた鍵生成アルゴリズムをそれぞれ特定できないようにすることにより、コンテンツ情報の不正な再生、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報復号化方法、復号化装置を提供すること。
【解決手段】　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリズムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を暗号化した暗号化第１の鍵のもとになる情報と、前記所定の鍵生成アルゴリズムを特定するためのアルゴリズム特定情報と、前記初期値を示す初期値情報とを用いてコンテンツ情報を復号する。

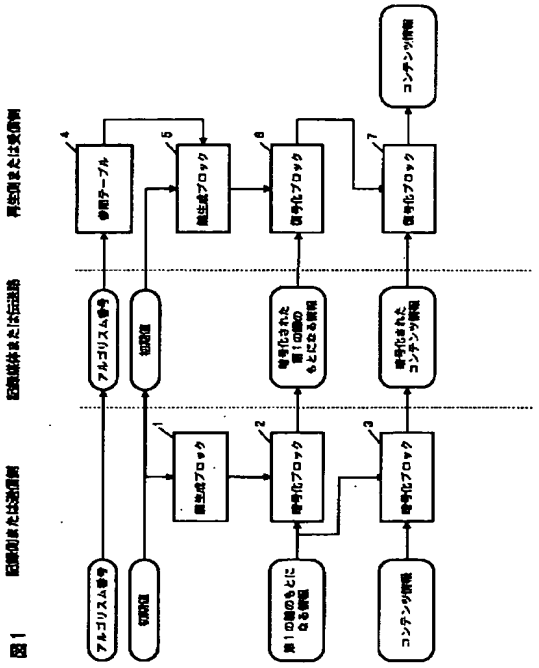


図１

【特許請求の範囲】

【請求項１】第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を暗号化した暗号化第１の鍵のもとになる情報と、
前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、
前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化方法であって、
前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定し、
前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリスムにより前記第２の鍵を生成し、
その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得、
この第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得る、ことを特徴とするコンテンツ情報復号化方法。

【請求項２】第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を暗号化した暗号化第１の鍵のもとになる情報と、
前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、
前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化装置であって、
前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定すると共に、前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリスムにより前記第２の鍵を生成する第２の鍵生成手段と、
その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得る第１の鍵情報復号化手段と、
この復号された第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得るコンテンツ情報復号化手段と、を設けたことを特徴とするコンテンツ情報復号化装置。

【請求項３】請求項２記載のコンテンツ情報復号化装置において、
前記第２の鍵生成手段は、複数の鍵生成アルゴリスムを備え、その複数の鍵生成アルゴリスムの中から前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定することを特徴とするコンテンツ情報復号化装置。

【請求項４】請求項３記載のコンテンツ情報復号化装置において、
前記第２の鍵生成手段における前記複数の鍵生成アルゴリスムはそれぞれ異なる原始多項式に基づくものであり、前記第２の鍵生成手段は、前記アルゴリスム特定情報により特定した所定の鍵生成アルゴリスムにおける原始多項式に従って、フィードバックの対象となるレジスタ位置を設定可能な線形フィードバックシフトレジスタを備えたことを特徴とするコンテンツ情報復号化装置。

【請求項５】第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を部分的に暗号化した暗号化第１の鍵のもとになる情報と、
前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、
前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化方法であって、
前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定し、
前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリスムにより前記第２の鍵を生成し、
その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得、
この第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得る、ことを特徴とするコンテンツ情報復号化方法。

【請求項６】第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を部分的に暗号化した暗号化第１の鍵のもとになる情報と、
前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、
前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化装置であって、
前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定すると共に、

前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリズムにより前記第２の鍵を生成する第２の鍵生成手段と、
その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得る第１の鍵情報復号化手段と、
この復号された第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得るコンテンツ情報復号化手段と、を設けたことを特徴とするコンテンツ情報復号化装置。

【請求項７】請求項６記載のコンテンツ情報復号化装置において、
前記第２の鍵生成手段は、複数の鍵生成アルゴリズムを備え、その複数の鍵生成アルゴリズムの中から前記アルゴリズム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリズムを特定することを特徴とするコンテンツ情報復号化装置。

【請求項８】請求項７記載のコンテンツ情報復号化装置において、
前記第２の鍵生成手段における前記複数の鍵生成アルゴリズムはそれぞれ異なる原始多項式に基づくものであり、前記第２の鍵生成手段は、前記アルゴリズム特定情報により特定した所定の鍵生成アルゴリズムにおける原始多項式に従って、フィードバックの対象となるレジスタ位置を設定可能な線形フィードバックシフトレジスタを備えたことを特徴とするコンテンツ情報復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ鍵とそのコンテンツ鍵を用いて暗号化された暗号化コンテンツ情報を再生（復号）するコンテンツ情報復号化方法、及び復号化装置に関するものである。そして、この発明は特に、処理速度の点で有利な対称暗号化のみを用いた場合においても、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報復号化方法、及び復号化装置を提供することを目的としている。

【０００２】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディジタルデータを配信する有用な方法として、特開平１０－２６９２８９のディジタルコンテンツ配布管理方法、ディジタルコンテンツ再生方法及び装置がある。この発明では、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信する。そして、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。

【０００３】また、特開平１０－２８３２６８の情報記記録媒体、記録装置、情報伝送システム、暗号解読装置では、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーして不正使用をすることを防止しするようにしている。

【０００４】暗号化方式は共通鍵を用いる対称暗号化方式と公開鍵、秘密鍵を用いる非対称暗号化方式に大別される。特開平１０－２８３２６８に示されるように、オーディオやビデオ等の大容量のディジタルデータ（コンテンツ情報）を伝送する場合、コンテンツ情報については共通鍵（コンテンツ鍵）を設定し、処理速度の点で有利な対象暗号化を行うと共に、用いたコンテンツ鍵について別途非対称暗号化を行って伝送する方法がある。しかしながら非対称暗号化は主に処理速度の大きさが欠点として挙げられる。このため、暗号化装置と復号化装置に共通な上位の鍵、いわゆるマスター鍵を設定し、コンテンツ鍵をさらにマスター鍵を用いて対称暗号化し伝送する方法も良く用いられる。

【０００５】

【発明が解決しようとする課題】しかしながら、上記の対称暗号化のみを用いる従来の方式では、暗号化装置を作成する側と復号化装置を作成する側において、暗号化方式に関する知識が一致してしまう。つまり、いずれの装置を作成する場合でもマスター鍵、コンテンツとコンテンツ鍵の暗号化アルゴリズムを知っていることが前提条件になると言うことである。このことは、暗号化装置を構成する知識で復号化装置を構成することが不可能ではないことを意味し、暗号化の目的である不正なコピーを防止し著作権を保護するという目的にそぐわない不正な復号化装置が流通する恐れがあった。

【０００６】本発明は、処理速度の点で有利な対称暗号化のみを用いた場合においても、暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリズム番号に従って暗号化に用いた鍵生成アルゴリズムをそれぞれ特定できないようにし、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とするコンテンツ情報復号化方法、及び復号化装置を提供することを目的としている。

【０００７】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記の方法・装置を提供するものである。

（１）　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を暗号化した暗号化第１の鍵のもとになる情報と、前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化方法であって、前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定し、前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリスムにより前記第２の鍵を生成し、その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得、この第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得る、ことを特徴とするコンテンツ情報復号化方法。

（２）　第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、与えられた初期値に基づき所定の鍵生成アルゴリスムにより生成された第２の鍵を用いて、前記第１の鍵のもとになる情報を暗号化した暗号化第１の鍵のもとになる情報と、前記所定の鍵生成アルゴリスムを特定するためのアルゴリスム特定情報と、前記初期値を示す初期値情報と、を用いて前記コンテンツ情報を復号する復号化装置であって、前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定すると共に、前記初期値情報から前記初期値を得て、この初期値を用いて前記特定された所定の鍵生成アルゴリスムにより前記第２の鍵を生成する第２の鍵生成手段と、その生成された第２の鍵により前記暗号化第１の鍵のもとになる情報を復号化して前記第１の鍵のもとになる情報を得る第１の鍵情報復号化手段と、この復号された第１の鍵のもとになる情報から前記第１の鍵を生成し、この第１の鍵により前記暗号化コンテンツ情報を復号化して前記コンテンツ情報を得るコンテンツ情報復号化手段と、を設けたことを特徴とするコンテンツ情報復号化装置。

（３）　上記（２）記載のコンテンツ情報復号化装置において、前記第２の鍵生成手段は、複数の鍵生成アルゴリスムを備え、その複数の鍵生成アルゴリスムの中から前記アルゴリスム特定情報により前記第２の鍵生成に用いた前記所定の鍵生成アルゴリスムを特定することを特徴とするコンテンツ情報復号化装置。

（４）　上記（３）記載のコンテンツ情報復号化装置において、前記第２の鍵生成手段における前記複数の鍵生成アルゴリスムはそれぞれ異なる原始多項式に基づくものであり、前記第２の鍵生成手段は、前記アルゴリスム特定情報により特定した所定の鍵生成アルゴリスムにおける原始多項式に従って、フィードバックの対象となるレジスタ位置を設定可能な線形フィードバックシフトレジスタを備えたことを特徴とするコンテンツ情報復号化装置。

【０００８】

【発明の実施の形態】図１に本発明のコンテンツ情報復号化装置の一実施例の概略構成を示す。なお、本説明においては、磁気記録媒体、光記録媒体、半導体メモリ等を記録媒体と呼び、光ケーブル、電線、無線伝送路等の信号を伝送する伝送媒体を伝送路と呼ぶこととする。

【０００９】まず、記録側または送信側について説明する。記録側または送信側においては、第２の鍵を生成するための鍵生成ブロック１、第１の鍵（コンテンツ鍵）のもとになる情報を前記第２の鍵により暗号化する暗号化ブロック２、及び、第１の鍵（コンテンツ鍵）のもとになる情報から第１の鍵（コンテンツ鍵）を生成してコンテンツ情報の暗号化を行う暗号化ブロック３を備えている。

【００１０】記録側または送信側の装置への入力は、

・再生側または受信側において第２の鍵生成のための鍵生成アルゴリスムの指定に用いられる、鍵生成ブロック１内で用いられる鍵生成アルゴリスムに対応したアルゴリスム番号と、

・鍵生成ブロック１に与えられる初期値と、

・コンテンツ情報の暗号化に用いられる第１の鍵（コンテンツ鍵）を生成するための第１の鍵のもとになる情報と、

・コンテンツ情報と、である。

【００１１】鍵生成ブロック１の出力である第２の鍵は、第１の鍵（コンテンツ鍵）のもとになる情報を暗号化するための上位鍵の役割を果たし、ランダムかつ初期値によって大きく変化することが求められる。

【００１２】図２に鍵生成ブロック１の一実施例を示す。この実施例においては、所定のビット数N(図例においてN=8)であるシフトレジスタ（ｒ１～ｒ８）と所定のレジスタ位置からの排他的論理和を得るためのゲート群（ｇ１～ｇ８）、係数設定バス及び初期値設定バスから構成されている。排他的論理和の結果を最下位レジスタへセットするこのような回路はリニアフィードバックシフトレジスタ(LFSR)と呼ばれている。初期値入力が初期値バスを通じて各レジスタにセットされると共に、係数入力によって各ゲートのスイッチ状態がセットされる。この後にシフトレジスタにクロックを与え、最上位レジスタからの出力を得る。

【００１３】最も効果的にランダムな出力を得るために

は設定係数がN次の原始多項式に対応していることが必要である。例えばN=8においては8次の原始多項式の1つである、

【００１４】

【数１】

数１

$$x^8 + x^7 + x^2 + x + 1$$

【００１５】を用いた場合、(g8, g7, g6, g5, g4, g3, g2, g1)に対応して係数(1, 1, 0, 0, 0, 0, 1, 1)が各ゲートに入力される。さらに初期値設定は値0以外が選択される。最上位レジスタからの出力はM系列と呼ばれる、高いランダム性を有したビット列となるが、LFSRの性質上将来の出力に関する予測が容易であるので、乗算等の非線形性を有した関数による変換を出力に備えることが理想的である。この出力ビット列を所定のフォーマットで第１の鍵（コンテンツ鍵）のもとになる情報の暗号化に用いる。

【００１６】第１の鍵のもとになる情報の暗号化ブロック２、及びコンテンツ情報の暗号化ブロック３については、DES等の広く公知である暗号化アルゴリスムを用いることができる。なお、暗号化された第１の鍵のもとになる情報は、第１の鍵のもとになる情報が第２の鍵により全て暗号化されたものでもよいし、部分的に暗号化されたものでもよい。（例えば、暗号化された第１の鍵のもとになる情報は、第１の鍵のもとになる情報の内の特に重要な部分のみが暗号化され、他の部分は暗号化されていない状態のものでもよい。）

【００１７】記録媒体あるいは伝送路上へは、第２の鍵＊生成のための鍵生成アルゴリスムの指定に用いられるアルゴリスム番号、初期値、暗号化された第１の鍵のもとになる情報、暗号化されたコンテンツ情報が所定のフォーマットで記録あるいは伝送される。アルゴリスム番号は前記した特定の原始多項式に対して一意でなければならない。

【００１８】なお、初期値やアルゴリスム番号は所定の関数により変換されて記録あるいは伝送されるようにしてもよい。（再生側または受信側では所定関数の逆関数を用いて初期値やアルゴリスム番号を得る。）

【００１９】次に、再生側または受信側について説明する。復号化装置は、第２の鍵生成のための鍵生成アルゴリスムを特定するための参照テーブル４、第２の鍵生成のための鍵生成ブロック５、第１の鍵（コンテンツ鍵）のもとになる情報の復号化ブロック６、及び、復号された第１の鍵のもとになる情報から第１の鍵（コンテンツ鍵）を生成してコンテンツ情報を復号するの復号化ブロック７を備えている。鍵生成ブロック５は記録側または送信側装置におけるものと同様の構成とする。第１の鍵（コンテンツ鍵）のもとになる情報の復号化ブロック６、及びコンテンツ情報の復号化ブロック７については、記録側または送信側装置の暗号化ブロック２及び３とそれぞれ対を成す構成とする。

【００２０】参照テーブル４は、アルゴリスム番号から第２の鍵生成のための原始多項式を特定するために設けられている。参照テーブル４は具体的にはROMで実現され、アルゴリスム番号を入力アドレスとして原始多項式に対応した係数列を出力として得るものである。原始多項式を8次とした場合の参照テーブルの構成例を表１に示す。復号化装置の動作を以下に説明する。

【００２１】

【表１】

表１ 参照テーブルの一例

アルゴリスム番号	係数列	原始多項式
0	(1, 1, 0, 0, 0, 0, 1, 1)	$x^8 + x^7 + x^2 + x + 1$
1	(1, 0, 0, 0, 1, 1, 1, 0)	$x^8 + x^4 + x^3 + x^2 + 1$
2	(1, 0, 1, 1, 0, 1, 0, 0)	$x^8 + x^6 + x^5 + x^3 + 1$
3	(1, 1, 1, 1, 0, 0, 1, 1)	$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
4	(1, 0, 0, 1, 0, 1, 0, 1)	$x^8 + x^5 + x^3 + x + 1$
5	(1, 0, 1, 1, 0, 0, 1, 0)	$x^8 + x^6 + x^5 + x^2 + 1$
6	(1, 0, 1, 1, 0, 0, 0, 1)	$x^8 + x^6 + x^5 + x + 1$
7	(1, 0, 1, 0, 1, 1, 1, 1)	$x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$

【００２２】復号化装置は、記録媒体あるいは伝送路からのアルゴリスム番号を参照テーブル４へ入力し、対応する係数列を得る。この係数列と記録媒体あるいは伝送路からの初期値を鍵生成ブロック５へ入力し、記録側または送信側と同様にレジスタへの初期値のセットとゲート状態のセットを行った後にクロックを与えて出力のビット列を得る。出力ビット列は所定のフォーマットで第１の鍵（コンテンツ鍵）のもとになる情報の復号化鍵として用いられ、復号化ブロック６において記録媒体あるいは伝送路からの情報を第１の鍵（コンテンツ鍵）のも

とになる情報へ復号化する。さらに、この復号された第１の鍵のもとになる情報から第１の鍵（コンテンツ鍵）を生成して、記録媒体あるいは伝送路からの暗号化コンテンツ情報を復号化ブロック７において復号化する。

【００２３】実施にあたっては、暗号化強度保持の観点から復号化装置全体が解析等を受け難いように実現されることが望ましい。特に、参照テーブル４は復号化装置の外部に内容が読み出される可能性が低くなるような配慮が必要である。好適な実施方法としては復号化装置全体を一体のLSIとすることである。

【００２４】このように、本実施例では、参照テーブル４が復号化側のみに与えられるため、暗号化側に与えられる知識のみでは指定されたアルゴリスム番号に従って鍵生成アルゴリスムを変更する機能を持った復号化装置を作成することが不可能である。よって、懸念される不正な復号化装置が作成されることを防止する効果がある。さらに、暗号化段階で用いられている鍵生成アルゴリスムのみを実現している不正な復号化装置が発見された場合、暗号化側で鍵生成アルゴリスムを変更すると同時に伝送するアルゴリスム番号を変更することで、不正な復号化装置での復号化が不可能なコンテンツの配信、配布を可能とする。

【００２５】なお、上記実施例の記録または伝送装置、及び復号化装置においては、第１の鍵（コンテンツ鍵）のもとになる情報と鍵生成ブロックが出力する上位鍵（第２の鍵）を用いると共に暗号化、復号化ブロックが2段となっている例を示したが、第１の鍵（コンテンツ鍵）のもとになる情報をM個用意し、第１の鍵（コンテンツ鍵）のもとになる情報の暗号化をM段としてもよい。この場合は媒体または伝送路上で、M個の暗号化第１の鍵のもとになる情報が記録、伝送されることになる。

【００２６】

【発明の効果】以上のように、本発明によれば、処理速度の点で有利な対称暗号化のみを用いた場合においても、暗号化側に与えられる知識のみでは、復号化側において、指定された各アルゴリスム番号に従って暗号化に用いた鍵生成アルゴリスムをそれぞれ特定できないようにすることにより、コンテンツ情報の不正な再生（復号）、コピーをより強力に防止し著作権保護の強化を可能とする。

【図面の簡単な説明】

【図１】本発明の一実施例の概略構成を示す図である。

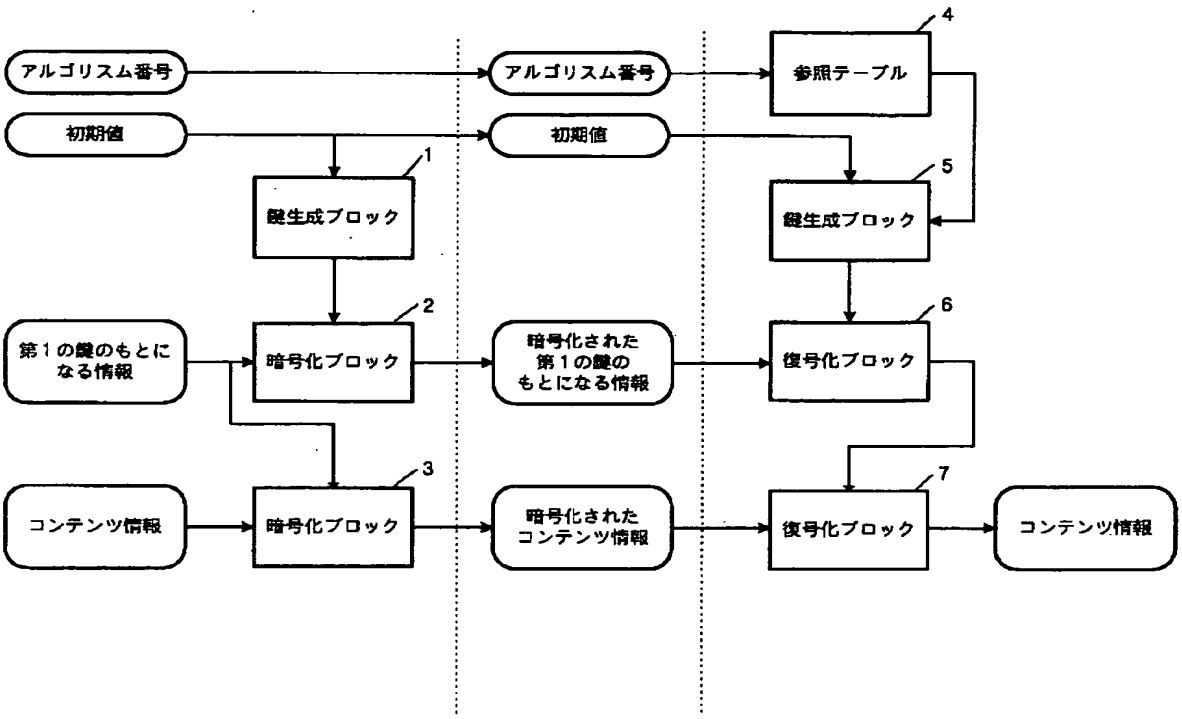
【図２】記録側または送信側の鍵生成ブロックの一例を示す図である。

【符号の説明】

１，５　鍵生成ブロック
２，３　暗号化ブロック
４　参照テーブル
６，７　復号化ブロック

【図１】

図１


記録側または送信側
記録媒体または伝送路
再生側または受信側
アルゴリスム番号
アルゴリスム番号
参照テーブル
4
初期値
初期値
1
鍵生成ブロック
5
鍵生成ブロック
第１の鍵のもとになる情報
2
暗号化ブロック
暗号化された第１の鍵のもとになる情報
6
復号化ブロック
3
コンテンツ情報
暗号化ブロック
暗号化されたコンテンツ情報
7
復号化ブロック
コンテンツ情報

【図２】

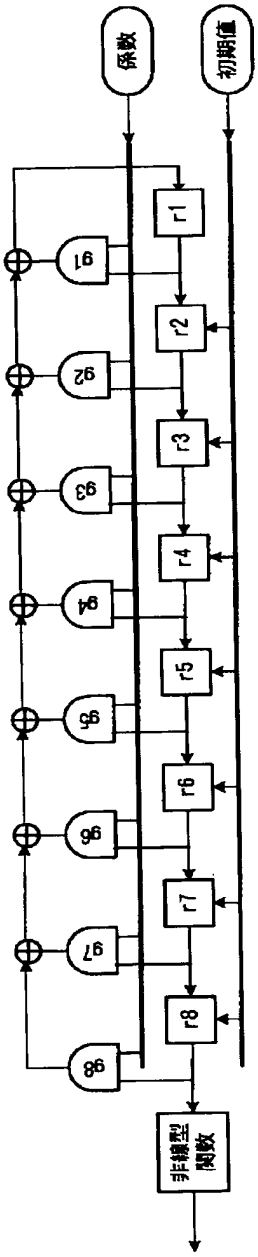


図２　　鍵生成ブロックの実施例

フロントページの続き

(72)発明者　上田　健二朗
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　日暮　誠司
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考) 5J104 AA07 AA16 DA04 EA06 EA18
JA03 KA04 MA05 NA02 NA08
PA07 PA14
9A001 EE03 LL03